REMARKS

Claim 12 was found objectionable because of a misspelling of "fourth". This has been corrected above (by a change to "sixth program instructions").

Claims 17-20 have been canceled, and claims 21-24 have been added.

Claims 1-12 were rejected under 35 USC 101 because, in the words of the Examiner, "there is no mention of the program instructions being embodied on [to the medium]". These claims originally recited that the program instructions are "recorded" on the medium, and have been amended to recite that the program instructions are "embodied" on the medium.

Claims 1-2, 4-5 and 13-15 were rejected under 35 USC 102 based on US Patent Publication 2003/0145228 to Suuronen et al. Claims 3, 8-11, 18 and 20 were rejected under 35 USC 103 based on Suuronen et al in view of Grenot. Applicants respectfully traverse this rejection based on the following.

Claim 1 recites a computer program product for automatically determining if a packet is a new, exploit candidate. First program instructions determine if the packet is a known exploit or portion thereof. Second program instructions determine if the packet is addressed to a broadcast IP address of a network. Third program instructions determine if the packet is network administration traffic. Fourth program instructions are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of the network, or network administration traffic, to determine that the packet is not a new, exploit candidate. Fifth program instructions are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of the network, network administration traffic or another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate.

Suuronen et al. disclose a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams (packets called the "first type" in Suuronen et al.), which cannot be viruses and should bypass the virus scanning engine. The objective is to avoid the overhead and delays involved in virus screening of audio and video data streams, which need to reach their destination in real time, and are not viruses. Suuronen et al. also state that packets of the "first type" include "other real time data which cannot contain viruses are not delayed by the virus scanning engine." However, Suuronen et al. fail to disclose the second and third program instructions of claim 1 which determine if the packet is addressed to a broadcast IP address of a network or network administrative traffic. Suuronen et al. fail to disclose the fourth program instructions of claim 1 which are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of the network, or network administration traffic, to determine that the packet is not a new, exploit candidate. Suuronen et al. fail to disclose the fifth program instructions which are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of the network, network administration traffic or another type of traffic known to be benign, to determine and report that the packet is a new exploit candidate.

Also, Suuronen et al. do not teach or suggest identification of new, exploit candidates as specified in the fourth and fifth program instructions of claim 1. Rather, Suuronen et al. merely determine which packets should be passed to a virus scanning engine "with virus detection criteria specified by virus detection database 24." See Suuronen et al. Paragraph 0021. Thus, Suuronen et al. determine if the packets contain a known virus signature. If a packet passes through the virus scanning engine of Suuronen, this means that the packet is presumed not to be a virus. The virus scanning engine of Suuronen et al. does not attempt to identify new, exploit candidates that do not exist in the virus detection database.

Grenot does not fill the gap of Suuronen et al. Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot discloses that an identification signature for each data packet is calculated. Grenot also discloses that "each packet is subjected to a classification operation 44. Criteria for classification are typically those that are conventionally retained to identify flows between networks and sub-networks (such as IP network subaddresses), flows between end equipment (such as IP addresses), flows between applications (such as IP addresses and UDP/TCP transport addresses), etc. Each packet is then identified by combining all or part of the elements: class, date signature." Column 6 lines 26-34. However, Grenot does not disclose or even suggest a program for determining new, exploit candidates. Rather, Grenot is concerned with measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot does not disclose any algorithm for determining new, exploit candidates. Grenot does not disclose the algorithm of claim 1 for determining new, exploit candidates. Even though Grenot identifies various IP addresses associated with a packet, Grenot does not perform the program operations of claim 1 to determine new, exploit candidates. Grenot fail to disclose program instructions of claim 1 which determine whether a packet is a new, exploit candidate based on whether the packet is a known exploit or portion thereof, addressed to a broadcast IP address of the network or network administration traffic.

Claims 2-12 depend on claim 1, and therefore, distinguish over the prior art for the same reasons as claim 1.

Independent claim 13 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover. Claims 14-16 depend on claim 13, and therefore, distinguish over the prior for the same reasons as claim 13.

New, independent claim 21 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover. In addition, claim 21 recites another criteria to determine whether the packet is a new, exploit candidate, i.e. whether the packet has a protocol listed in a list of protocols assumed to be harmless broadcast traffic. Claims 22-24 depend on claim 21, and therefore, distinguish over the prior art for the same reasons that claim 21 distinguishes thereover.

Dependent claims 2, 11, 14 and 22 recite another criteria for determining if the packet is a new, exploit candidate, i.e. whether it is web crawler traffic.

Based on the foregoing, the present patent application as amended above should be allowed.

Respectfully submitted,

Dated: 01/05/07
Telephone: 607-429-4368
Fax No.: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297